Deutscher Bundestag **Drucksache 19/10137**

19. Wahlperiode 14.05.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Margarete Bause, Agnieszka Brugger, Jürgen Trittin, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 19/9523 –

Deutsch-Chinesischer Cyberkonsultationsmechanismus

Vorbemerkung der Fragesteller

Anlässlich der vierten deutsch-chinesischen Regierungskonsultationen am 13. Juli 2016 haben sich Deutschland und die Volksrepublik China auf die Schaffung eines Cyberkonsultationsmechanismus verständigt. Dieses Dialogformat fand erstmalig am 17. Mai 2018 in Peking statt und soll laut Bundesministerium des Innern, für Bau und Heimat (BMI) jährlich wiederholt werden.

Formuliertes Ziel künftiger Konsultationen ist es, sich auf Regierungsebene bilateral über aktuelle legislative Entwicklungen im Bereich der IT-Gesetzgebung und entsprechende Auswirkungen auf Unternehmen und Institutionen auszutauschen. Infolge des ersten Mechanismus wurde auch die Einrichtung einer Kontaktstelle für den anlassbezogenen schnellen Austausch von Informationen zur Cybersicherheitslage, zu Entwicklungen im Bereich der IT-Kriminalität, Sabotage und zur Bekämpfung von terroristischen Aktivitäten vereinbart.

Die Bundesregierung muss nach Ansicht der Fragesteller diesen Dialog nutzen, um den Herausforderungen des digitalen Zeitalters menschen- und bürgerrechtsorientiert sowie rechtsstaatlich zu begegnen. Für mehr Sicherheit und Freiheit im digitalen Raum braucht es nach Ansicht der Fragesteller einen glaubwürdigen Einsatz für internationale Regeln und gegen eine Militarisierung des Netzes. Internationale Regelungen, die es Staaten erlauben, unter dem Deckmantel der IT-Sicherheit Zensur zu betreiben und Menschen zu verfolgen, muss die Bundesregierung entschieden zurückweisen.

Eine neue Aktualität und erhöhte öffentliche Aufmerksamkeit der zu verhandelnden Themen hat sich auch durch die sehr intensive öffentliche Debatte um die Rolle chinesischer Firmen wie Huawei beim 5G-Ausbau in Deutschland und eine durch die Bundesregierung in diesem Kontext in Aussicht gestellte Änderung des Telekommunikationsgesetzes (TKG) sowie ein durch die Bundesregierung immer wieder debattiertes, sogenanntes „No-Spy-Abkommen“ mit der Volksrepublik China ergeben. Ziel dieses No-Spy-Abkommens ist es, die chinesische Seite zu verpflichten, der deutschen Seite Garantien bezüglich der Nichtanwendung rechtlicher Vorgaben zu geben, die chinesische Anbieter zu einer weitreichenden Kooperation mit dem chinesischen Staat verpflichten

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 10. Mai 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

(vgl. www.golem.de/news/tkg-aenderung-regierung-plant-angeblich-knebelgesetz-fuer-huawei-1902-139360.html; www.wiwo.de/politik/deutschland/sicherheitskreise-merkel-will-anti-spionageabkommen-mit-china/24046378.html).

Wie bezüglich der genauen Ausgestaltung des deutsch-chinesischen Cyberkonsultationsmechanismus besteht auch bezüglich dieser durch die Bundesregierung angekündigten Vorhaben derzeit nach Ansicht der Fragesteller noch eine erhebliche Unklarheit, was den aktuellen Verhandlungsstand sowohl innerhalb der Bundesregierung als auch mit den chinesischen Partnern sowie was die genaue Ausgestaltung der jeweiligen Regelungen angeht.

Cyberkonsultationsmechanismus

1. Wer hat am vergangenen deutsch-chinesischen Cyberkonsultationsmechanismus teilgenommen (bitte Personen inkl. Funktion bzw. Zuständigkeit bzw. Referatszugehörigkeit für beide Seiten auflisten)?

   Falls keine detaillierten Informationen über die chinesischen Teilnehmenden vorliegen, welche Sicherheitsbehörden und andere staatliche Stellen waren von chinesischer Seite aus beteiligt?

Dr. Günter Krings, Parlamentarischer Staatssekretär beim Bundesminister des Innern, für Bau und Heimat, hat die deutsche Delegation geleitet. Darüber hinaus haben teilgenommen:

- BMI: Abteilungsleiter der Abteilung Cyber- und Informationssicherheit, Referat ITI2 (Referatsleitung, Mitarbeiter), Büro des Parlamentarischen Staatssekretärs Dr. Günter Krings (Mitarbeiterin),
- BMWi: Unterabteilungsleiterin VI A, Referat VI A 5 (Mitarbeiter),
- AA: Referat AP01 (Referatsleitung), Botschaft Peking (Gesandter, Leiter der Rechts- und Konsularabteilung, zwei Referenten der Wirtschaftsabteilung, Dolmetscherin).

Der Vizeminister SHI Jun, Ministerium für öffentliche Sicherheit (MöS), hat die chinesische Delegation geleitet. Darüber hinaus haben Vertreter folgender Einrichtungen teilgenommen:

- Chinesische Botschaft in Berlin
- Kommission für Politik und Recht
- Cyberspace Administration of China (CAC)
- Ministerium für Industrie und Informationstechnologie (MIIT)
- Chinesisches Wirtschaftsministerium
- Chinesisches Außenministerium

2. Was war der genaue Gegenstand der Verhandlungen beim letzten Cyberkonsultationsmechanismus zwischen der Bundesrepublik Deutschland und der Volksrepublik China?

Beide Seiten haben sich über den Stand der Cybergesetzgebung und die Auswirkung auf die Wirtschaft informiert und sich über Nutzen und Notwendigkeit von geschützten Virtual-Private-Network-Verbindungen (VPN-Verbindungen) ausgetauscht. Die deutsche Seite hat ihr Interesse am Austausch zur Standardisierung und Zertifizierung im Bereich der Digitalisierung dargestellt. Beide Seiten haben sich über die aktuelle Lage der Cyberkriminalität in beiden Ländern ausgetauscht.

3. Hat die Bundesregierung im Zuge vergangener Konsultationsmechanismen die menschenrechtlichen und bürgerrechtlichen Folgen und Implikationen folgender Themen angesprochen, und falls ja, mit welchem Ziel, und welchem jeweiligen Ergebnis:

   a) Entwicklung der IT-Gesetzgebung;

   b) Privacy by Design; Security by Design;

   c) digitale Infrastruktur;

   d) Export von digitaler Infrastruktur in Drittstaaten;

   e) Anonymisierungsdienste wie etwa Tor zum Schutz von Nichtregierungsorganisationen und Menschenrechtsverteidigerinnen und Menschenrechtsverteidigern;

   f) lizenzfreier VPN-Einsatz zum Schutz von Nichtregierungsorganisationen und Menschenrechtsverteidigerinnen und Menschenrechtsverteidigern;

   g) Social-Scoring-Systeme; Export von Social-Scoring-Systemen;

   h) ethische Aspekte von KI-Anwendungen;

   i) Militarisierung des Netzes?

Die Bundesregierung hat in der nur wenige Stunden dauernden und als Auftaktveranstaltung gedachten Besprechung die menschenrechtlichen und bürgerrechtlichen Fragen insbesondere in Bezug auf eine sichere Nutzung von VPN-Tunneln im Zuge des deutsch-chinesischen Cyberkonsultationsmechanismus angesprochen.

4. Hat die Bundesregierung darüber hinaus menschenrechtliche Folgen und Implikationen weiterer Themen, die Bestandteil des Cyberkonsultationsmechanismus waren, thematisiert (bitte auflisten, welche weiteren Themen angesprochen wurden und welche konkreten Ergebnisse es jeweils hierzu gab)?

Nein.

5. Wurden beim vergangenen Cyberkonsultationsmechanismus gemeinsame Aktionen gegen Dritte thematisiert?

   Wenn ja, welche?

Nein.

6. Gab es vor, während oder nach dem deutsch-chinesischen Cyberkonsultationsmechanismus vom 17. Mai 2018 gemeinsam durchgeführte Aktionen gegen Dritte, und wenn ja, aus welchen Gründen, und gegen wen (bitte inklusive der Art der Aktion und der erfolgten Zusammenarbeit – z. B. Informationsaustausch, technische Bereitstellung o. Ä. – möglichst konkret auflisten)?

Nein.

7. Gab es im Rahmen des deutsch-chinesischen Cyberkonsultationsmechanismus vom 17. Mai 2018 einen Austausch über kritische Infrastrukturen beispielsweise hinsichtlich eines verbesserten Schutzes oder von (gemeinsamen) Frühwarnsystemen?

   Wenn ja, mit welchen Ergebnissen?

Nein.

8. Welche schriftlichen Dokumente sind während und nach Abschluss des ersten Cyberkonsultationsmechanismus entstanden (z. B. gemeinsame Erklärung; Memorandum of Understanding; Pressemitteilungen; Protokolle; Berichte zur internen Nutzung in den Ministerien; Sachstände, Korrespondenzen zwischen und innerhalb der Ministerien; Drahtberichte; Berichte der deutschen Botschaft Peking; Non-Paper etc.)?

Außer der durch die Fragesteller bereits erwähnten Pressemitteilung vom 18. Mai 2018 wurden keine weiteren abschließenden Dokumente erstellt.

Im Übrigen wird auf die Antwort zu Frage 9 verwiesen.

9. Welche Erkenntnisse hat die Bundesregierung aus dem Cyberkonsultationsmechanismus vom 17. Mai 2018 gezogen?

   Ist insbesondere die Organisation und der Ablauf der Konsultation evaluiert worden?

   Falls ja, welche Veränderungen ergeben sich daraus für weitere Cyberkonsultationsmechanismen?

Es bestehen Unterschiede in der Wahrnehmung der zu behandelnden Themen auf deutscher und chinesischer Seite, welche die Einigung auf den Themenumfang des Cyberkonsultationsmechanismus erschweren. Dies hat bisher auch die Erstellung einer konsentierten Abschlusserklärung verhindert. Vereinbart wurde ein jährliches Treffen auf St-Ebene abwechselnd in Berlin und Peking. Aufgrund der weiterhin bestehenden Differenzen hinsichtlich der zu behandelnden Themen, sind zunächst weitere Abstimmungsgespräche notwendig. Der Hauptschwerpunkt liegt aus deutscher Sicht auf den wirtschaftspolitischen Auswirkungen der chinesischen Cybersicherheitsgesetzgebung.

10. Inwiefern plant die Bundesregierung im Rahmen des Cyberkonsultationsmechanismus mit China eine gemeinsame Verständigung – beispielsweise in Form eines Code of Conduct – über das Vorgehen im Rahmen nachrichtendienstlicher, militärischer oder sonstiger Aufklärung?

Auf die Antwort zu Frage 9 wird verwiesen.

11. Wann und wo soll der zweite deutsch-chinesische Cyberkonsultationsmechanismus stattfinden?

Die Terminverhandlungen laufen derzeit.

12. Wer wird am zweiten deutsch-chinesischen Cyberkonsultationsmechanismus teilnehmen (bitte Personen inkl. Funktion bzw. Zuständigkeit bzw. Referatszugehörigkeit auflisten)?

Eine Gesprächsführung auf St-Ebene ist vorgesehen. Die sonstige Teilnahme ist abhängig von der noch abzustimmenden Agenda.

13. Welche Themen plant die Bundesregierung beim bevorstehenden, zweiten deutsch-chinesischen Cyberkonsultationsmechanismus schwerpunktmäßig anzusprechen, und aus welchen Gründen misst sie diesen eine besondere Bedeutung bei?

Das Themenspektrum künftiger Konsultationsmechanismen bezieht sich aus Sicht der Bundesregierung auf den anlassbezogenen schnellen Austausch von Informationen zur Cybersicherheitslage in den Bereichen Cyberkriminalität, Cybersabotage und Bekämpfung von terroristischen Aktivitäten im Cyberraum. Des Weitern soll aus Sicht der Bundesregierung ein bilateraler Austausch über die aktuellen Entwicklungen der Cybergesetzgebung und ihre Auswirkungen auf Unternehmen und Institutionen stattfinden.

14. Plant die Bundesregierung weiterhin (vgl. Antwort zu Frage 5 der Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 18/1802), menschenrechtliche und bürgerrechtliche Themen beim bevorstehenden, zweiten deutsch-chinesischen Cyberkonsultationsmechanismus zur Sprache zu bringen, und falls ja, welche, und in welcher konkreten Form?

Im Rahmen des Cyberkonsultationsmechanismus ist die Behandlung dieser Themen nicht vorgesehen. Es wird darauf hingewiesen, dass es sich bei den in der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/ DIE GRÜNEN auf Bundestagsdrucksache 18/1802 angesprochenen Cyberkonsultationen um ein anderes Gesprächsformat handelt.

15. Plant die Bundesregierung, beispielsweise im Rahmen des nächsten Konsultationsmechanismus, sich auch mit chinesischen Menschenrechtsaktivistinnen und Menschenrechtsaktivisten, Journalistinnen und Journalisten und/ oder Bloggerinnen und Bloggern auszutauschen?

Es wird auf die Antwort zu Frage 14 verwiesen.

16. In welchen weiteren Formaten tauscht sich die Bundesregierung mit China über aktuelle Entwicklungen der IT- Gesetzgebung und deren Auswirkungen auf Unternehmen, Institutionen und die Zivilgesellschaft aus, und wie wird für den Informations- und Wissenstransfer zwischen diesen Formaten Sorge getragen?

Die Bundesregierung tauscht sich mit China in folgenden weiteren Formaten aus:

- bilaterale Gespräche auf Minister-, Staatssekretärs- und Abteilungsleiterebene;
- Kooperation Industrie 4.0
- DE-CHN Jahrestagung zu Industrie 4.0
- DE-CHN Arbeitsgruppe Unternehmen zu Industrie 4.0
- Konferenz zu Industrie 4.0 auf Hannover Messe 2019

17. Gibt es derzeit oder gab es in der Vergangenheit einen vergleichbaren Mechanismus mit anderen Staaten?

    a) Wenn ja, mit welchen Staaten wurden entsprechende Mechanismen durchgeführt (bitte nach Staaten getrennt auflisten), wie oft wurden diese durchgeführt, wann wurden diese erstmalig durchgeführt und in welchem Zeitraum wurden bzw. werden diese wiederholt bzw. weshalb wurde sich gegen eine Wiederholung entschieden?

    b) Wenn nein, ist eine Ausweitung dieses Mechanismus auf andere Staaten geplant?

       Falls ja, auf welche Staaten soll dieser Mechanismus ausgeweitet werden?

       Gibt es bereits konkrete Planungen?

       Was ist beispielsweise mit Staaten, die durchaus ähnliche gesetzliche Mitwirkungsverpflichtungen von Unternehmen und Staatsbürgern haben (vgl. beispielsweise: www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal/komplettansicht), Sicherheitsbehörden und Geheimdiensten bei der Kompromittierung von informationstechnischen Systemen aktiv zu helfen?

       Falls nein, warum nicht?

Mit anderen Staaten gab und gibt es keinen vergleichbaren Mechanismus. Die Ausweitung vergleichbarer Mechanismen auf andere Staaten ist derzeit nicht geplant.

18. Gibt es nach Kenntnis der Bundesregierung, im Rahmen der verstärkten Konsolidierung der europäischen Positionierung gegenüber China, Überlegungen, einen ähnlichen Cyberkonsultationsmechanismus auf europäischer Ebene zu etablieren?

Die Europäische Union hat der Regierung der Volksrepublik China vorgeschlagen, im Rahmen der bereits bestehenden „EU-China Cyber Taskforce“ eine Arbeitsgruppe einzurichten, die sich dem Schutz geistigen Eigentums gegen böswillige Cyberaktivitäten widmet. Eine Antwort von chinesischer Seite steht derzeit noch aus.

Kontaktstelle

19. Wann wurde die Kontaktstelle für den anlassbezogenen, schnellen Austausch von Informationen zur Cybersicherheitslage in den Bereichen IT-Kriminalität, Sabotage und Bekämpfung von strafrechtlichen Aktivitäten online auf deutscher sowie auf chinesischer Seite eingerichtet, und wann haben diese ihre Arbeit aufgenommen (vgl. Pressemitteilung des BMI vom 18. Mai 2018)?

20. Mit welchen Personal- und Finanzmitteln ist die deutsche Kontaktstelle ausgestattet?

    a) Besitzt die Bundesregierung Kenntnis darüber, mit welchen Personal- und Finanzmitteln die chinesische Kontaktstelle ausgestattet ist?

       Falls ja, mit welchen Personal- und Finanzmitteln ist die chinesische Kontaktstelle ausgestattet?

    b) Welche Personen und Organisationseinheiten sind auf deutscher Seite in die Kontaktstelle eingebunden (Staatssekretäre, Parlamentarische Staatssekretäre, Sonderbeauftragte, Abteilungen, Unterabteilungen, Referate, deutsche Botschaft etc.; bitte möglichst konkret auflisten)?

21. Welche Befugnisse hat die deutsche Kontaktstelle und auf welcher Ebene ist sie angesiedelt?

    a) Besitzt die Bundesregierung Kenntnis darüber, auf welcher Ebene die chinesische Kontaktstelle angesiedelt ist und welche Befugnisse diese besitzt?

    Falls ja, auf welcher Ebene ist die chinesische Kontaktstelle angesiedelt, und welche Befugnisse besitzt diese?

22. Welche Voraussetzungen müssen erfüllt sein, damit die Kontaktstelle für den anlassbezogenen, schnellen Austausch von Informationen zur Cybersicherheitslage in den Bereichen IT-Kriminalität, Sabotage und Bekämpfung von strafrechtlichen Aktivitäten im IT-Raum eingeschaltet wird?

23. Ist eine Zusammenarbeit der Kontaktstelle mit anderen bestehenden Einrichtungen mit ähnlichem Themenspektrum wie beispielsweise dem Cyberabwehrzentrum (CAZ) geplant, und, sollte dies der Fall sein, wie sind die genauen Modalitäten der Zusammenarbeit ausgestaltet?

Die Fragen 19 bis 23 werden zusammen beantwortet.

Die Kontaktstelle für den anlassbezogenen, schnellen Austausch von Informationen zur Cybersicherheitslage in den Bereichen Cyberkriminalität, Cybersabotage und Bekämpfung von terroristischen Aktivitäten im Cyberraum wurde noch nicht eingerichtet.

24. Ist die Bundesregierung der Ansicht, dass die bestehenden Strukturen und Mechanismen ausreichen, um neue hybride Bedrohungslagen zu erkennen, oder bedarf es nach Ansicht der Bundesregierung, auch und gerade vor dem Hintergrund weitreichender IT-Angriffe, Hacks, Leaks, Doxing-Fälle, intransparenten Beeinflussungen demokratischer Willensbildungsprozesse und gezielten Desinformationskampagnen, neuer Strukturen, um auf diese hybriden Bedrohungslagen angemessen reagieren zu können?

Die Bundesregierung ist entsprechend sensibilisiert und beobachtet insbesondere, aber nicht ausschließlich durch ihre Sicherheitsbehörden alle Aktivitäten, die hybride Bedrohungslagen darstellen könnten, um lageangepasst zu reagieren.

25. Gibt es Möglichkeiten, dass Unternehmen, Institutionen oder zivilgesellschaftliche Akteure (z. B. NGOs), um die Kontaktstelle für den Austausch anzurufen oder Themen aufzusetzen?

    Wenn ja, welche (bitte sofern unterschiedliche Voraussetzungen für Unternehmen, Institutionen oder zivilgesellschaftliche Akteure vorliegen, getrennt auflisten)?

26. Wie viele Kontaktaufnahmen gab es seit Arbeitsaufnahme bis zur Einreichung dieser Anfrage bei der Kontaktstelle, und auf welche Themen bezogen sich diese Anfragen (bitte nach chinesischen und deutschen Anfragen getrennt auflisten)?

27. Auf welche Weise stellt die Bundesregierung sicher, dass Anfragen zur Cybersicherheitslage, zur IT-Kriminalität, zur Sabotage oder zur Bekämpfung von strafrechtlichen Aktivitäten im IT-Raum nicht dafür missbraucht werden, um Schutzbedürftige (z. B. Journalistinnen und Journalisten, Bloggerinnen und Blogger, Menschenrechtsaktivistinnen und Menschenrechtsaktivisten oder religiöse Minderheiten wie die Uigurinnen und Uiguren) zu verfolgen?

28. Gibt es eine Diskrepanz zwischen Auskunftsersuchen und erteilten Auskünften?

    Falls ja, wie viele Auskunftsersuchen wurden von chinesischer Seite nicht beantwortet, und aus welchen Gründen geschah dies?

    Wie viele Auskunftsersuchen wurden von deutscher Seite nicht beantwortet, und aus welchen Gründen geschah dies (bitte so detailliert wie möglich, mindestens aber themenbezogen auflisten)?

Die Fragen 25 bis 28 werden zusammen beantwortet.

Es wird auf die Antwort zu Frage 19 verwiesen.

TKG-Änderung, No-Spy-Abkommen und Europäische Perspektive

29. Wie ist der aktuelle Stand bezüglich der von der Bundesregierung angekündigten Änderungen des Telekommunikationsgesetzes (TKG), um der staatlichen Verantwortung zum Schutz digitaler Infrastrukturen zukünftig gerecht zu werden, und gibt es bereits einen entsprechenden Kriterienkatalog?

    Falls ja, was genau ist der Regelungsgegenstand?

    Falls nein, warum nicht?

Die Bundesregierung plant im Rahmen der Überarbeitung des Sicherheitskataloges nach § 109 Absatz 6 des Telekommunikationsgesetzes (TKG) u. a., dass sicherheitsrelevante Netz- und Systemkomponenten (kritische Kernkomponenten) nur nach einer geeigneten Abnahmeprüfung bei Zulieferung eingesetzt werden dürfen sowie regelmäßig Sicherheitsprüfungen unterzogen werden müssen. Die Definition der sicherheitsrelevanten Komponenten (kritische Kernkomponenten) erfolgt einvernehmlich zwischen der Bundesnetzagentur (BNetzA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Dabei wird auch eine Differenzierung zwischen Kern- und Zugangsnetz zu prüfen sein. Die Arbeiten an den geplanten Änderungen des Sicherheitskataloges sind noch nicht abgeschlossen.

30. Wer genau ist innerhalb der Bundesregierung derzeit mit der Arbeit an der von der Bundesregierung angekündigten Änderung des Telekommunikationsgesetztes (TKG) beschäftigt (bitte möglichst konkret nach Bundesministerien, Abteilungen etc. auflisten)?

Im Rahmen der laufenden Novelle des Telekommunikationsgesetzes zur Umsetzung der Vorgaben der Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation werden alle fachlich betroffenen Ressorts beteiligt. Federführend zuständig für diesen Prozess ist innerhalb der Bundesregierung das Bundesministerium für Wirtschaft und Energie gemeinsam mit dem Bundesministerium für Verkehr und digitale Infrastruktur.

31. Wie will die Bundesregierung gewährleisten, dass die von der Bundesregierung angekündigten Änderungen des Telekommunikationsgesetzes (TKG) mit der ebenfalls seit langem in Aussicht gestellten Vorlage eines IT-Sicherheitsgesetzes 2.0 korrespondieren, und wann ist mit der Vorlage des IT-Sicherheitsgesetzes 2.0 zu rechnen?

Gesetzgebungsvorhaben der Bundesregierung werden koordiniert bearbeitet. Der Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme wird derzeit innerhalb der Bundesregierung abgestimmt.

32. Wie ist der derzeitige Stand bezüglich der Verhandlungen eines sogenannten No-Spy-Abkommens zwischen der Bundesrepublik Deutschland und der Volksrepublik China?

    Gab es bereits Vorgespräche oder Verhandlungen zu einem solchen Abkommen (falls ja, bitte mit Datum und Inhalt der Gespräche bzw. Verhandlungen auflisten)?

    Gibt es Überlegungen, solche Verhandlungen erneut aufzunehmen oder bereits bestehende Verhandlungen fortzuführen (vgl. Antwort auf die Schriftliche Frage 1 der Abgeordneten Margarete Bause auf Bundestagsdrucksache 19/7138)?

33. Was soll der genaue Gegenstand eines solchen No-Spy-Abkommens nach dem Willen der Bundesregierung sein?

34. Für wie groß hält die Bundesregierung, auch vor dem Hintergrund von Bemühungen des Abschlusses vergleichbarer Abkommen mit anderen Staaten in der Vergangenheit (vgl.: www.sueddeutsche.de/politik/no-spy-abkommen-geschichte-eines-taeuschungsmanoevers-1.2494417; vgl.: www.washingtonpost.com/world/national-security/the-us-and-china-agree-not-to-conduct-economic-espionage-in-cyberspace/2015/09/25/1c03f4b8-63a2-11e5-8e9e-dce8a2a2a679_story.html), die Bereitschaft der chinesischen Seite, ein solches Abkommen tatsächlich abzuschließen?

35. Welche konkreten Schritte hat die Bundesregierung wann unternommen, um zum Abschluss eines solchen Abkommens zu kommen, und was waren die Reaktionen der chinesischen Regierung auf die bisherigen Bemühungen?

36. Hätte der Abschluss eines No-Spy-Abkommens mit China Auswirkungen auf die bisherige sicherheitspolitische Bewertung chinesischer Produkte und Dienstleistungen durch die Bundesregierung?

    Falls ja, welche Veränderungen an chinesischen Produkten und Dienstleistungen erwartet die Bundesregierung?

37. Gibt es derzeit oder gab es in der Vergangenheit Bemühungen zum Abschluss vergleichbarer Abkommen mit anderen Staaten?

    a) Wenn ja, welche (bitte nach einzelnen Staaten und Abkommen auflisten)?

    b) Wenn nein, warum nicht?

Die Fragen 32 bis 37b werden zusammen beantwortet.

Es wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 1 der Abgeordneten Margarete Bause auf Bundestagsdrucksache 19/7138 sowie auf die Antwort der Bundesregierung auf die Schriftliche Frage 4 des Abgeordneten Uwe Schulz auf Bundestagsdrucksache 19/8660 verwiesen.

38. Wird die in Kürze in Kraft tretende EU-Verordnung zur „Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Union“ nach Auffassung der Bundesregierung zu einer Anpassung der Außenwirtschaftsverordnung (AWV) führen, sodass auch Komponentenausrüster in Bereichen kritischer Infrastruktur in den Anwendungsbereich der Investitionsprüfung fallen,

    a) und wie beurteilt die Bundesregierung eine solche Erweiterung der AWV,

    b) und wenn nein, wird die Bundesregierung unabhängig von der EU-Verordnung eine solche Erweiterung anstreben?

Die sektorübergreifende Investitionsprüfung nach den §§ 55 ff. der Außenwirtschaftsverordnung (AWV) erfasst bereits seit ihrer Einführung alle Erwerbe inländischer Unternehmen durch unionsfremde Investoren, unabhängig davon, in welchem Geschäftsbereich die Unternehmen tätig sind. Gleichermaßen erfasst sind alle Erwerbe von Anteilen an inländischen Unternehmen, durch die der unionsfremde Investor Kontrolle über ein bestimmtes Mindestquorum an Stimmrechten erlangt. Dies gilt auch für Komponentenausrüster in Bereichen kritischer Infrastrukturen. Prüfmaßstab ist, ob aus dem Erwerb eine Gefahr für die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland resultiert.

39. Wird die in Kürze in Kraft tretende EU-Verordnung zur „Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Union“ nach Auffassung der Bundesregierung zu einer Anpassung der Außenwirtschaftsverordnung (AWV) führen, sodass auch der Aufbau kritischer Infrastruktur im Rahmen der Investitionsprüfung überprüft werden kann,

    a) und wie bewertet die Bundesregierung eine solche Erweiterung der AWV,

    b) und wenn nein, wird die Bundesregierung unabhängig von der EU-Verordnung eine solche Erweiterung anstreben?

Die neue EU-Verordnung gilt für von unionsfremden Investoren getätigte Investition jeder Art zur Schaffung oder Aufrechterhaltung dauerhafter und direkter Beziehungen zwischen dem unionsfremden Investor und einem unionsangehörigen Unternehmen. Die bloße Neuerrichtung oder Erweiterung technischer Anlagen durch einen unionsfremden Investor wird nicht erfasst. Die Bundesregierung strebt keine über den Anwendungsbereich der EU-Verordnung hinaus greifende Geltung der sektorübergreifenden Investitionsprüfung an. Die Abwehr von Gefahren, die aus der Neuerrichtung oder Erweiterung technischer Anlagen durch einen unionsfremden Investor resultieren, ist Aufgabe des anlagenbezogenen Fachrechts.

40. Welche konkreten Aspekte der IT-Sicherheit wurden im Rahmen des EU-China Gipfels am 9. April 2019 diskutiert?

    a) Welche Rolle nahm dabei die Frage der Beteiligung chinesischer Firmen an der zu errichtenden 5G-Infrastruktur ein?

    b) Welche Rolle spielte dabei die Forderung der USA, die chinesische Firma Huawei von der Errichtung der 5G-Infrastruktur auszuschließen?

Beide Seiten sprachen IT-Sicherheit im Rahmen der Zusammenarbeit in der „EU-China Cyber Taskforce“ an. Über das Unternehmen Huawei wurde nicht gesprochen.

41. Welchen Einfluss auf die Sicherheitssituation in Deutschland hätte nach Kenntnis der Bundesregierung die von den USA angekündigte Einschränkung der Geheimdienstkooperation, wenn die Firma Huawei am 5G-Netzausbau beteiligt wird, und wie will die Bundesregierung diese Einschränkung kompensieren?

    Ist der Bundesregierung bekannt, ob ähnliche Drohungen seitens der USA an andere Regierungen von EU-Mitgliedstaaten gerichtet wurden?

    Wenn ja, welche?

    Wenn ja, gibt es einen Austausch zwischen den betroffenen Ländern zu dieser Problematik?

Die Bundesregierung sieht derzeit keine Einschränkung in der Kooperation mit den Vereinigten Staaten von Amerika.

Außer Medienberichten zum Thema liegen der Bundesregierung keine Erkenntnisse im Sinne der Frage vor.



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333